A PROJECT REPORT

ON

AWS Elastic Load Balancing Inside of a Virtual Private Cloud

Submitted to: ICT Academy (IITK)

Under the guidance of Amit Sir

Faculty (Cloud System Administration)

Submitted by: SHREY NIGAM

(Jaypee University of Engineering and Technology, Guna)

Id: 366360

Acknowledgement

The learning opportunity I had with ICT Academy was a great chance for learning and professional development. Therefore, I consider myself as a very lucky individual as I was provided with an opportunity to be a part of it. I am also grateful for having a chance to meet so many wonderful students who led me though this learning period.

It is my radiant sentiment to place on record my best regards, deepest sense of gratitude to Amit Sir Faculty (Cloud System Administration) for their careful and precious guidance which was extremely valuable for my study both theoretically and practically.

I perceive as this opportunity as a big milestone in my career development. I will strive to use gained skills and knowledge in the best possible way, and I will continue to work on their improvement, in order to attain desired career objectives. Hope to continue cooperation with all of you in the future,

Sincerely,

Shrey Nigam

Id: 366360

Jaypee University of Engineering and Technology

Introduction to Elastic Load Balancing and VPC:

Elastic Load Balancing is a technique that automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers (Application, Network and Classic Load Balancer) that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault tolerant.

AWS offers a variety of different infrastructure and platform services. Virtual Private Cloud is among one of them.

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

You can easily customize the network configuration of your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the internet. You can also place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. You can use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Benefits of Using AWS Load Balancer:

A load balancer distributes workloads across multiple compute resources, such as virtual servers. Using a load balancer increases the availability and fault tolerance of your applications.

You can add and remove compute resources from your load balancer as your needs change, without disrupting the overall flow of requests to your applications.

You can configure health checks, which monitor the health of the compute resources, so that the load balancer sends requests only to the healthy ones. You can also offload the work of encryption and decryption to your load balancer so that your compute resources can focus on their main work.

Accessing Elastic Load Balancing:

You can create, access, and manage your load balancers using any of the following interfaces:

- **AWS Management Console**— Provides a web interface that you can use to access Elastic Load Balancing.
- **AWS Command Line Interface (AWS CLI)** — Provides commands for a broad set of AWS services, including Elastic Load Balancing. The AWS CLI is supported on Windows, macOS, and Linux.
- **AWS SDKs** — Provide language-specific APIs and take care of many of the connection details, such as calculating signatures, handling request retries, and error handling.
- **Query API**— Provides low-level API actions that you call using HTTPS requests. Using the Query API is the most direct way to access Elastic Load Balancing.

Related Services (ELB):

Elastic Load Balancing works with the following services to improve the availability and scalability of your applications.

- **Amazon EC2** — Virtual servers that run your applications in the cloud. You can configure your load balancer to route traffic to your EC2 instances.
- **Amazon EC2 Auto Scaling** — Ensures that you are running your desired number of instances, even if an instance fails. Amazon EC2 Auto Scaling also enables you to automatically increase or decrease the number of instances as the demand on your instances changes.
- **AWS Certificate Manager** — When you create an HTTPS listener, you can specify certificates provided by ACM. The load balancer uses certificates to terminate connections and decrypt requests from clients.
- **Amazon CloudWatch** — Enables you to monitor your load balancer and to take action as needed.
- **Amazon ECS** — Enables you to run, stop, and manage Docker containers on a cluster of EC2 instances. You can configure your load balancer to route traffic to your containers.
- **AWS Global Accelerator** — Improves the availability and performance of your application. Use an accelerator to distribute traffic across multiple load balancers in one or more AWS Regions.
- **Route 53** — Provides a reliable and cost-effective way to route visitors to websites by translating domain names into the numeric IP addresses that computers use to connect to each other.
- **AWS WAF** — You can use AWS WAF with your Application Load Balancer to allow or block requests based on the rules in a web access control list (web ACL).

Benefits of Using Virtual Private Cloud:

Virtual private clouds offer a number of benefits for your business.

- Security – Since private clouds are built around one single business, the data storage, network, and hardware can be specifically designed around the security needs of your business. It cannot be accessed by any other client or company in the same building or data center.
- Compliance – Compliance is much easier to accomplish because each network and storage configuration is based around one single client. This makes it much easier to monitor their security and compliance needs.
- Customization – Network performance, storage performance, and hardware performance can be specifically customized into the client's private cloud.

Accessing Amazon VPC:

You can create, access, and manage your VPCs using any of the following interfaces:

- **AWS Management Console** — Provides a web interface that you can use to access your VPCs.
- **AWS Command Line Interface (AWS CLI)** — Provides commands for a broad set of AWS services, including Amazon VPC, and is supported on Windows, Mac, and Linux.
- **AWS SDKs** — Provides language-specific APIs and takes care of many of the connection details, such as calculating signatures, handling request retries, and error handling.
- **Query API** — Provides low-level API actions that you call using HTTPS requests.

Amazon VPC Concepts:

Amazon VPC is the networking layer for Amazon EC2The following are the key concepts for VPCs:

- **Virtual private cloud (VPC)** — A virtual network dedicated to your AWS account.
- **Subnet** — A range of IP addresses in your VPC.
- **Route table** — A set of rules, called routes, that are used to determine where network traffic is directed.
- **Internet gateway** — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.
- **VPC endpoint** — Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Prerequisites for learning this project are:

- Having basic knowledge of operating systems like Windows OS, Linux etc.
- As Visualization play a major role in AWS you need to have the understanding of it.
- Networking is an essential skill as all operations on cloud platform involves it.
- Understanding the difference between the Public and Private cloud.
- Last but not the least, you must have basic command over coding.

Using Elastic Load Balancing in your Amazon Virtual Private Cloud (Amazon VPC):

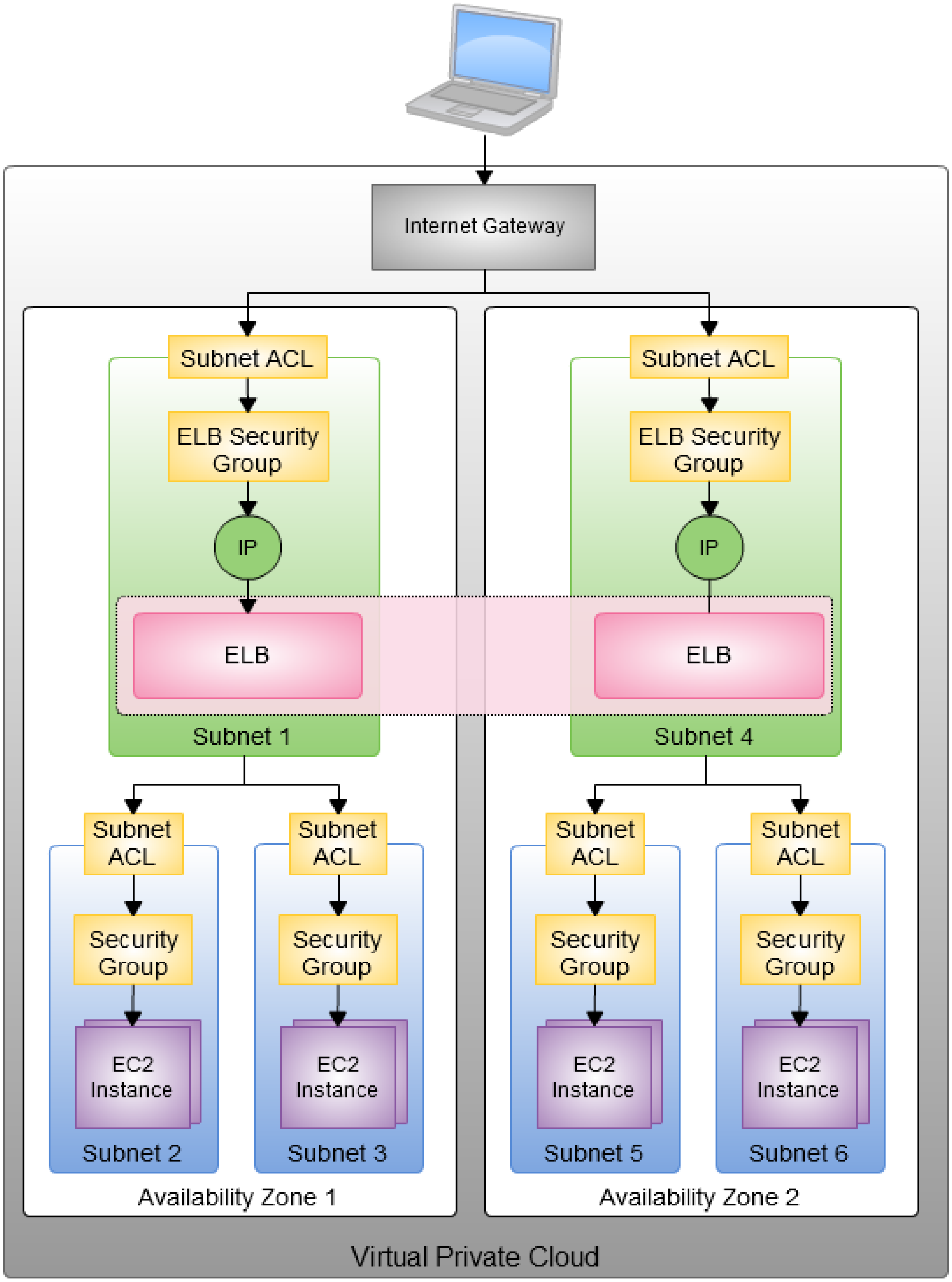
Elastic Load Balancing makes it easy to create an internet-facing entry point into your VPC or to route request traffic between tiers of your application within your VPC. You can assign security groups to your load balancer to control which ports are open to a list of allowed sources. Because Elastic Load Balancing is integrated with your VPC, all of your existing Network Access Control Lists (ACLs) and Routing Tables continue to provide additional network controls.

When you create a load balancer in your VPC, you can specify whether the load balancer is internet-facing (default) or internal. If you select internal, you do not need to have an internet gateway to reach the load balancer, and the private IP addresses of the load balancer will be used in the load balancer’s DNS record.

Elastic Load Balancing also allows you to use IP addresses to route requests to application targets. This offers you flexibility in how you virtualize your application targets, allowing you to host more applications on the same instance. This also enables these applications to have individual security groups and use the same network port to further simplify inter-application communication in microservice-based architecture.

Elastic Load Balancing also allows you to use IP addresses to route requests to application targets. This offers you flexibility in how you virtualize your application targets, allowing you to host more applications on the same instance. This also enables these applications to have individual security groups and use the same network port to further simplify inter-application communication in microservice-based architecture.

Design of the infrastructure, to be created for this project

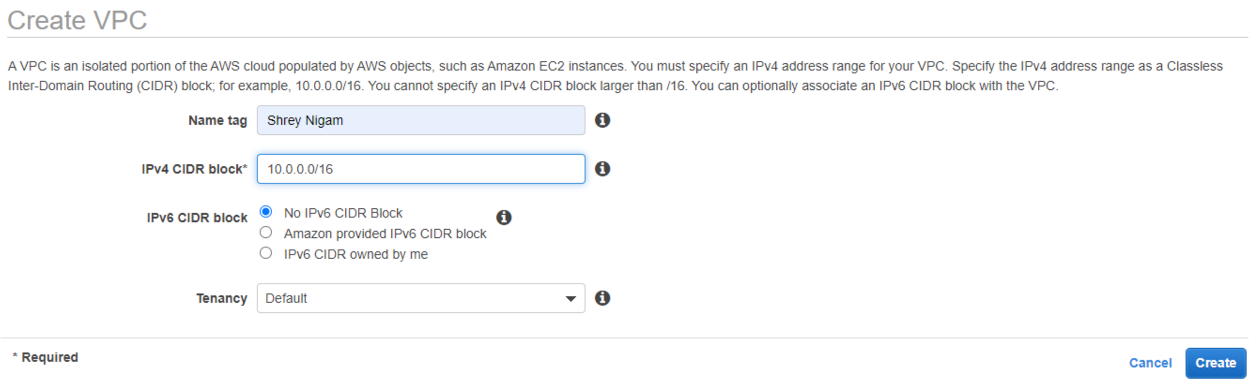


Setting up an Elastic Load Balancer inside a Virtual Private Cloud

Create an instance:

- Deploy a HTML page
- Create an AMI of that instance

Create a VPC:



Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

Name tag: Shrey Nigam

IPv4 CIDR block*: 10.0.0.0/16

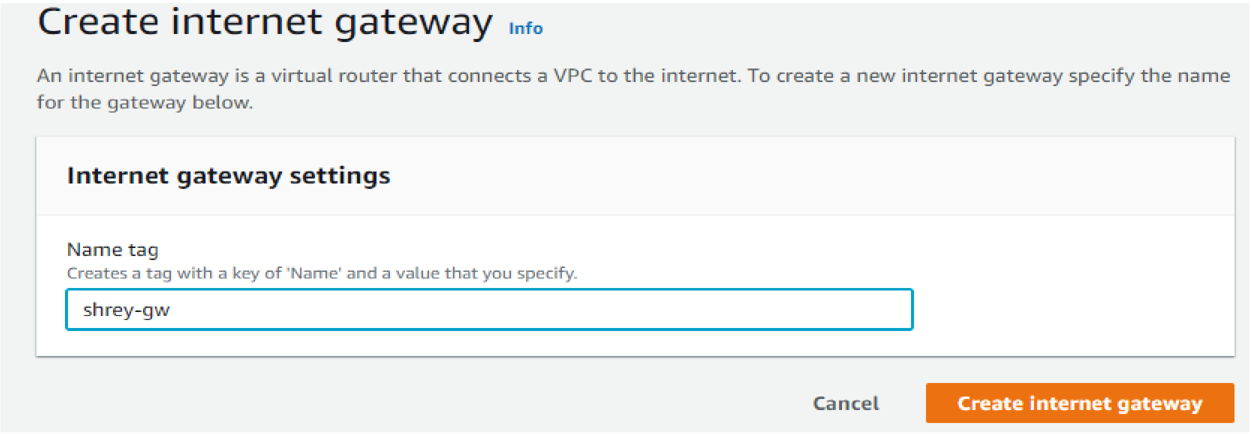
IPv6 CIDR block:
● No IPv6 CIDR Block
○ Amazon provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy: Default

* Required

Create Internet Gateway:

It acts as a virtual router that connects a vpc to the internet.



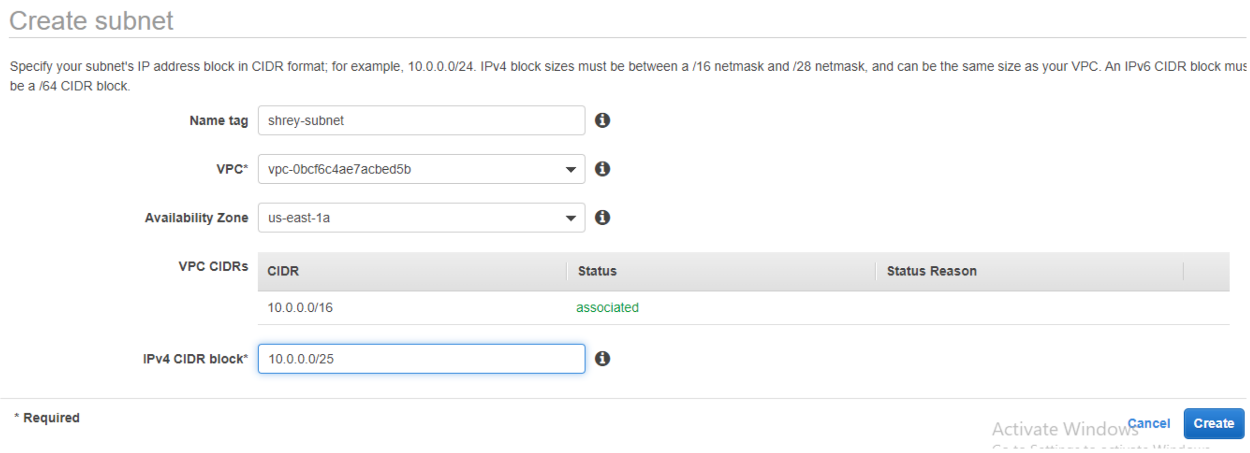
Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
shrey-gw

Create Subnets’:



Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block mus be a /64 CIDR block.

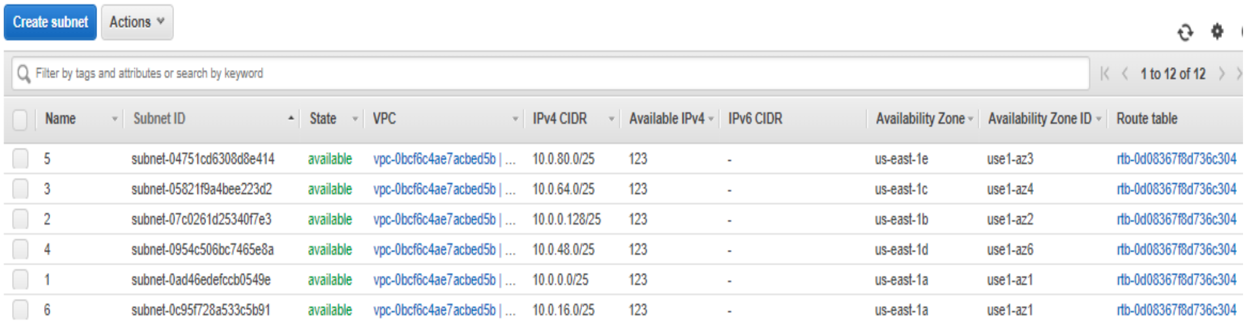
Name tag	shrey-subnet
VPC*	vpc-0bcf6c4ae7acbed5b
Availability Zone	us-east-1a
VPC CIDRs	
IPv4 CIDR block*	10.0.0.0/25

VPC CIDRs:

CIDR	Status	Status Reason
10.0.0.0/16	associated	

* Required

Create subnets for both required availability zones-



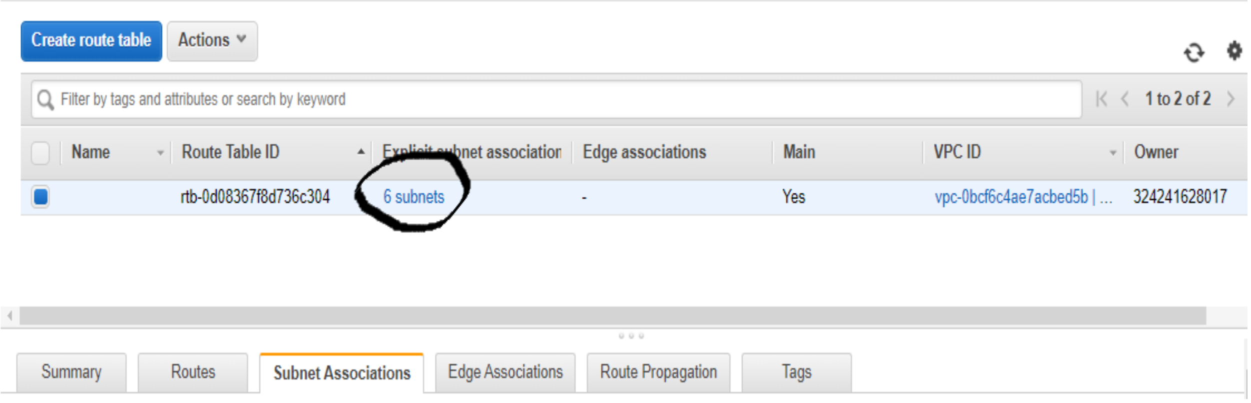
Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table
5	subnet-04751cd6308d8e414	available	vpc-0bcf6c4ae7acbed5b | ...	10.0.80.0/25	123	-	us-east-1e	use1-az3	rtb-0d08367f8d736c304
3	subnet-05821f9a4bee223d2	available	vpc-0bcf6c4ae7acbed5b | ...	10.0.64.0/25	123	-	us-east-1c	use1-az4	rtb-0d08367f8d736c304
2	subnet-07c0261d25340f7e3	available	vpc-0bcf6c4ae7acbed5b | ...	10.0.0.128/25	123	-	us-east-1b	use1-az2	rtb-0d08367f8d736c304
4	subnet-0954c506bc7465e8a	available	vpc-0bcf6c4ae7acbed5b | ...	10.0.48.0/25	123	-	us-east-1d	use1-az6	rtb-0d08367f8d736c304
1	subnet-0ad46edefccb0549e	available	vpc-0bcf6c4ae7acbed5b | ...	10.0.0.0/25	123	-	us-east-1a	use1-az1	rtb-0d08367f8d736c304
6	subnet-0c95f728a533c5b91	available	vpc-0bcf6c4ae7acbed5b | ...	10.0.16.0/25	123	-	us-east-1a	use1-az1	rtb-0d08367f8d736c304

Subnets are address blocks within your VPC to which you can assign different routes, ACLs, and appliances.

These ELB subnets are going to host the Application ELB's hosted instances. We still need to create the subnets that'll host your own application instances.

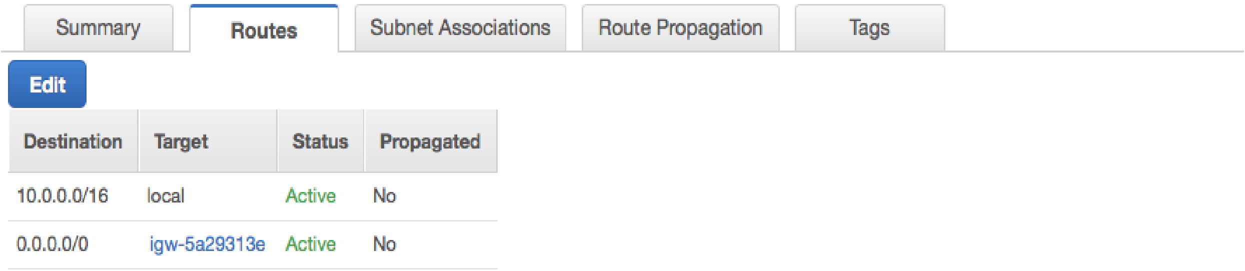
Create a Route Table:

and add inbound association-



Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
	rtb-0d08367f8d736c304	6 subnets	-	Yes	vpc-0bcf6c4ae7acbed5b | ...	324241628017

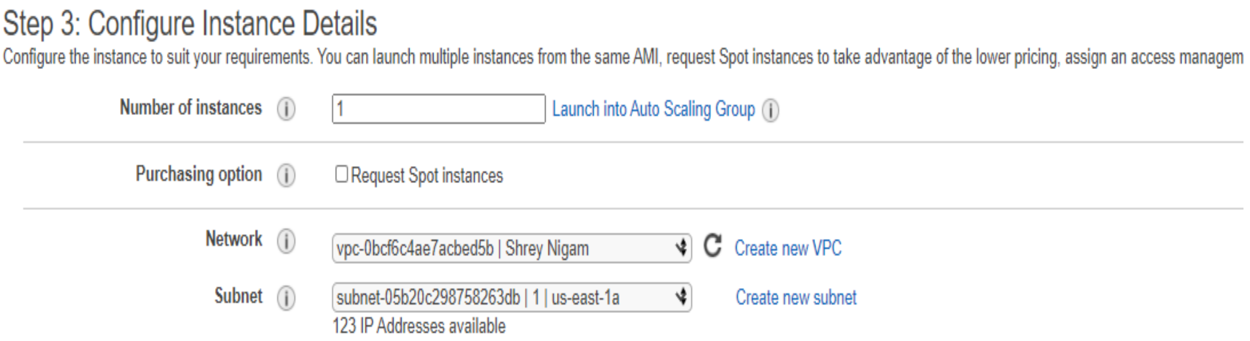
To make your ELB subnets Internet accessible - you have to associate your subnets to an Internet Gateway.



Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-5a29313e	Active	No

“An Internet gateway serves two purposes: to provide a target in your VPC route tables for Internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IP addresses.”

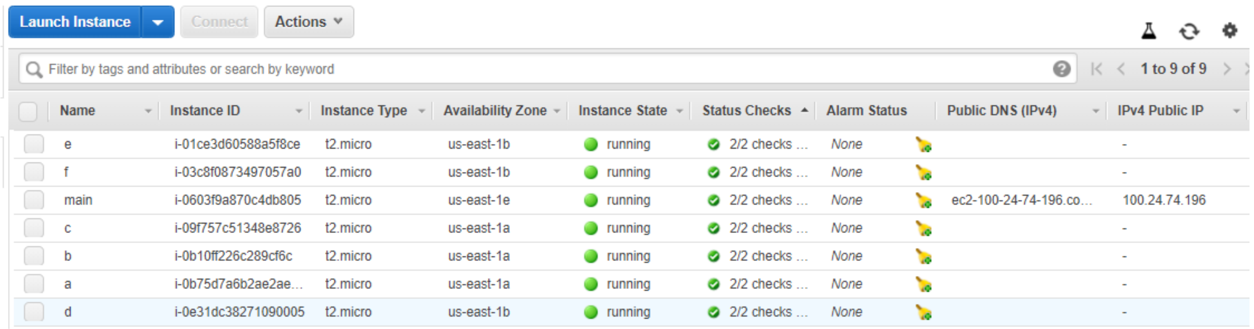
Configure AMI for VPC and Subnet:



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access managem

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-0bcf6c4ae7acbed5b | Shrey Nigam — Create new VPC
Subnet	subnet-05b20c298758263db | 1 | us-east-1a — Create new subnet 123 IP Addresses available

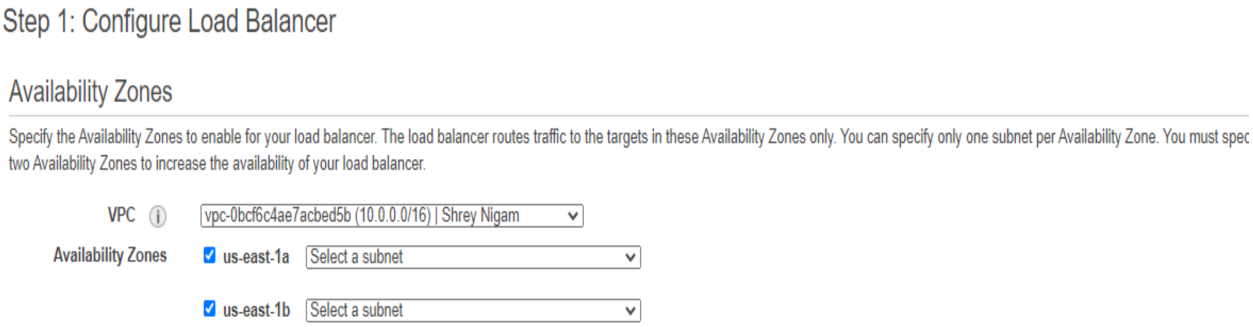


Filter by tags and attributes or search by keyword

1 to 9 of 9

□	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
□	e	i-01ce3d60588a5f8ce	t2.micro	us-east-1b	● running	✓ 2/2 checks ...	*None*		-
□	f	i-03c8f0873497057a0	t2.micro	us-east-1b	● running	✓ 2/2 checks ...	*None*		-
□	main	i-0603f9a870c4db805	t2.micro	us-east-1e	● running	✓ 2/2 checks ...	*None*	ec2-100-24-74-196.co...	100.24.74.196
□	c	i-09f757c51348e8726	t2.micro	us-east-1a	● running	✓ 2/2 checks ...	*None*		-
□	b	i-0b10ff226c289cf6c	t2.micro	us-east-1a	● running	✓ 2/2 checks ...	*None*		-
□	a	i-0b75d7a6b2ae2ae...	t2.micro	us-east-1a	● running	✓ 2/2 checks ...	*None*		-
□	d	i-0e31dc38271090005	t2.micro	us-east-1b	● running	✓ 2/2 checks ...	*None*		-

Configuring Load Balancer:



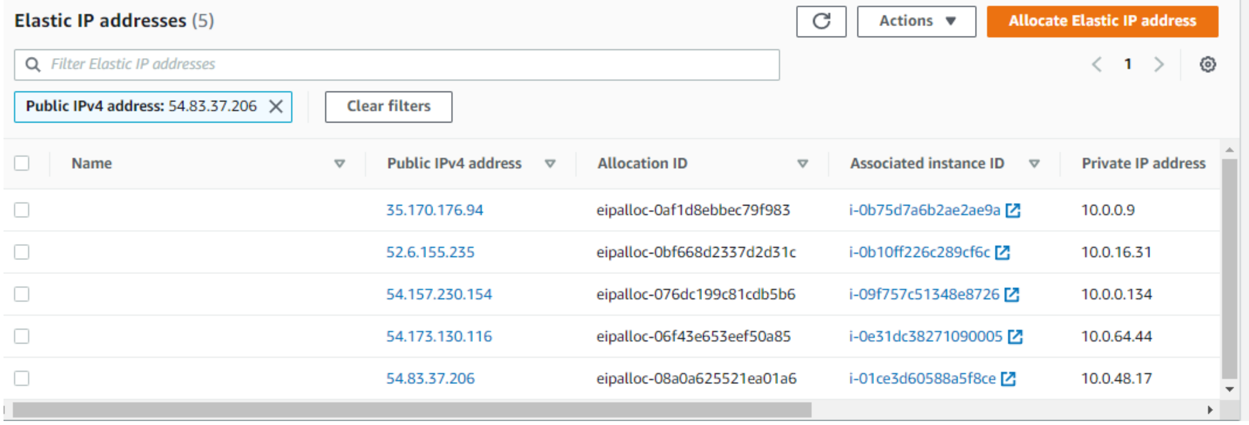
Step 1: Configure Load Balancer

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must spec two Availability Zones to increase the availability of your load balancer.

VPC	vpc-0bcf6c4ae7acbed5b (10.0.0.0/16) | Shrey Nigam
Availability Zones	☑ us-east-1a Select a subnet
	☑ us-east-1b Select a subnet

Allocate Elastic IP Address:



Elastic IP addresses (5)

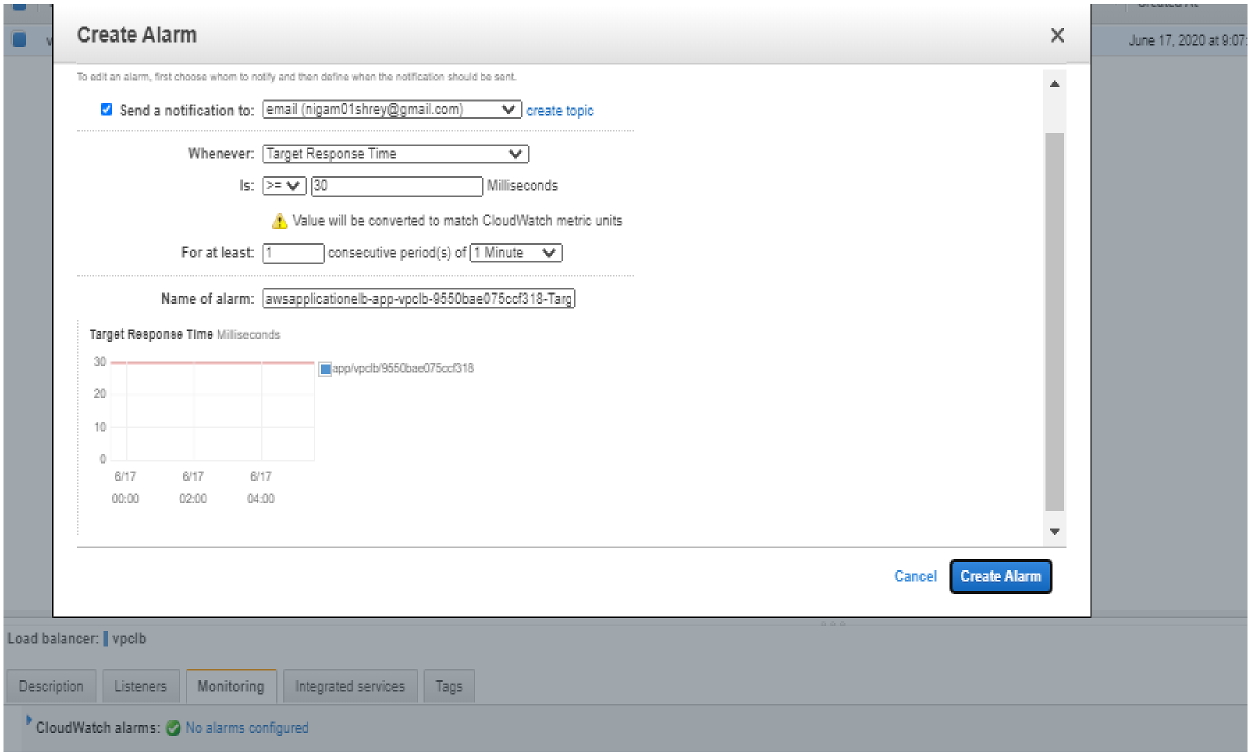
Filter Elastic IP addresses

Public IPv4 address: 54.83.37.206

□	Name	Public IPv4 address	Allocation ID	Associated instance ID	Private IP address
□		35.170.176.94	eipalloc-0af1d8ebbec79f983	i-0b75d7a6b2ae2ae9a	10.0.0.9
□		52.6.155.235	eipalloc-0bf668d2337d2d31c	i-0b10ff226c289cf6c	10.0.16.31
□		54.157.230.154	eipalloc-076dc199c81cdb5b6	i-09f757c51348e8726	10.0.0.134
□		54.173.130.116	eipalloc-06f43e653eef50a85	i-0e31dc38271090005	10.0.64.44
□		54.83.37.206	eipalloc-08a0a625521ea01a6	i-01ce3d60588a5f8ce	10.0.48.17

Create CloudWatch monitoring:

Amazon CloudWatch is a monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources.



Create Alarm

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☑ Send a notification to: email (nigam01shrey@gmail.com) create topic

Whenever: Target Response Time

Is: >= 30 Milliseconds

Value will be converted to match CloudWatch metric units

For at least: 1 consecutive period(s) of 1 Minute

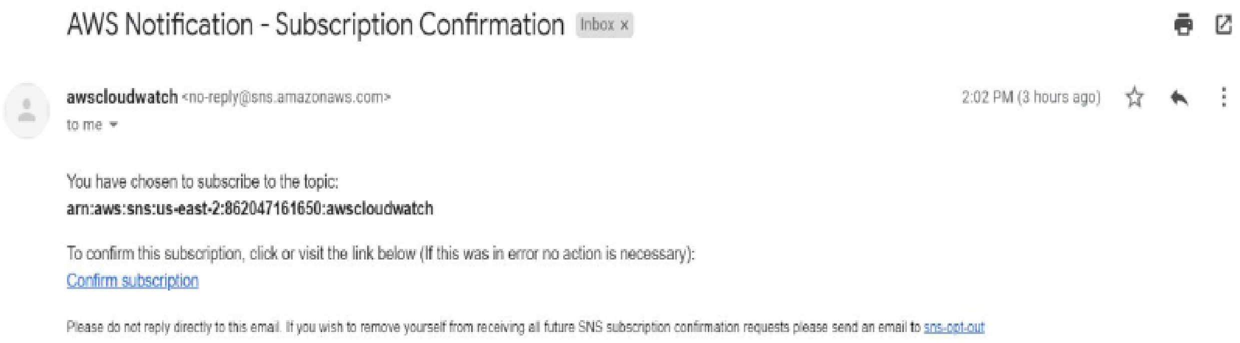
Name of alarm: awsapplicationelb-app-vpclb-9550bae075ccf318-Targ

Load balancer: vpclb

Description | Listeners | Monitoring | Integrated services | Tags

CloudWatch alarms: No alarms configured

Email notification for AWS CloudWatch monitoring:



AWS Notification - Subscription Confirmation

awscloudwatch <no-reply@sns.amazonaws.com>
to me

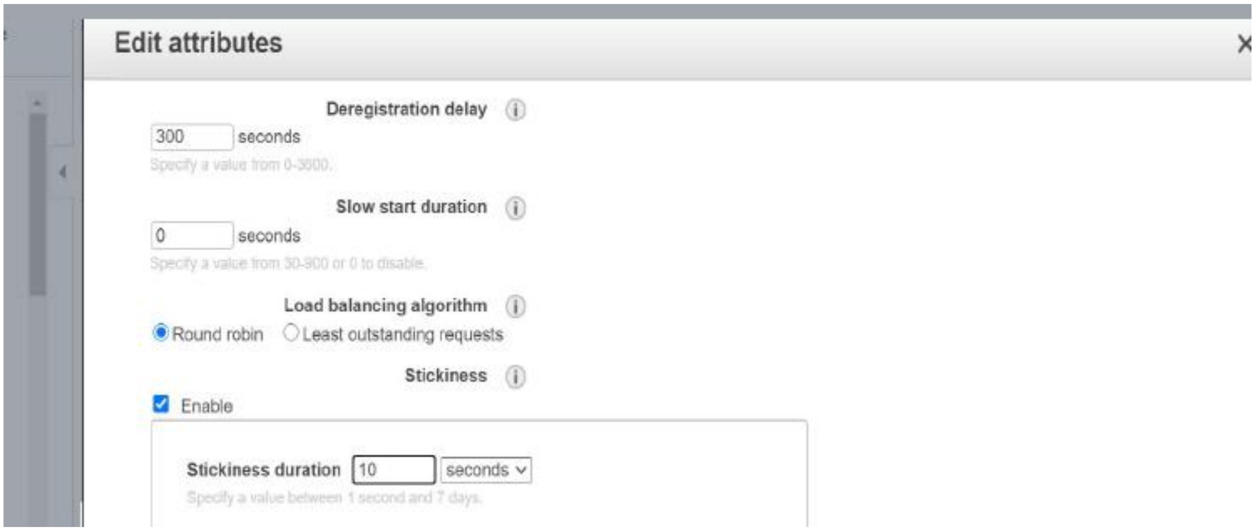
2:02 PM (3 hours ago)

You have chosen to subscribe to the topic:
arn:aws:sns:us-east-2:862047161650:awscloudwatch

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out

Configure Sticky Sessions:



Edit attributes

Deregistration delay
300 seconds
Specify a value from 0-3600.

Slow start duration
0 seconds
Specify a value from 30-900 or 0 to disable.

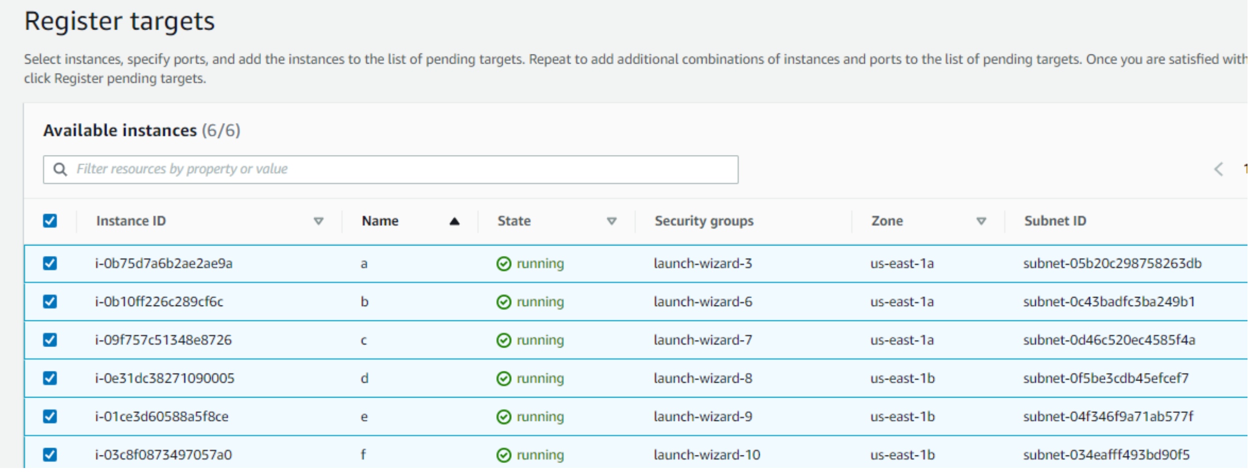
Load balancing algorithm
● Round robin ○ Least outstanding requests

Stickiness
☑ Enable

Stickiness duration 10 seconds
Specify a value between 1 second and 7 days.

Sticky sessions are a mechanism to route requests from the same client to the same target. Application **Load Balancer** supports **sticky sessions** using **load balancer** generated cookies. If you enable **sticky sessions**, the same target receives the request and can use the cookie to recover the **session** context.

Register Target Groups:



Register targets

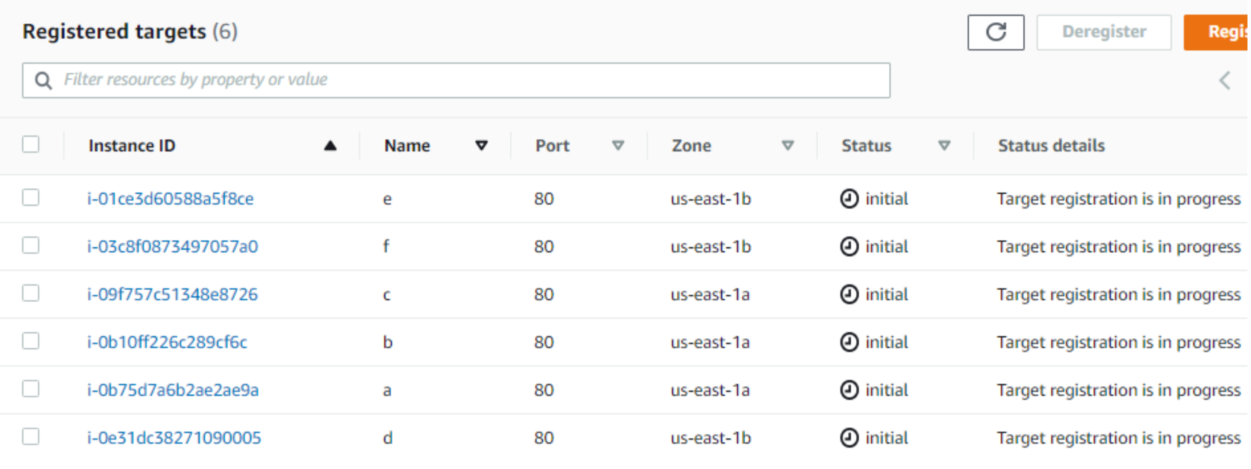
Select instances, specify ports, and add the instances to the list of pending targets. Repeat to add additional combinations of instances and ports to the list of pending targets. Once you are satisfied with click Register pending targets.

Available instances (6/6)

☑	Instance ID	Name	State	Security groups	Zone	Subnet ID
☑	i-0b75d7a6b2ae2ae9a	a	running	launch-wizard-3	us-east-1a	subnet-05b20c298758263db
☑	i-0b10ff226c289cf6c	b	running	launch-wizard-6	us-east-1a	subnet-0c43badfc3ba249b1
☑	i-09f757c51348e8726	c	running	launch-wizard-7	us-east-1a	subnet-0d46c520ec4585f4a
☑	i-0e31dc38271090005	d	running	launch-wizard-8	us-east-1b	subnet-0f5be3cdb45efcef7
☑	i-01ce3d60588a5f8ce	e	running	launch-wizard-9	us-east-1b	subnet-04f346f9a71ab577f
☑	i-03c8f0873497057a0	f	running	launch-wizard-10	us-east-1b	subnet-034eafff493bd90f5

Configure Health Checks for your Target Groups:

Before the load balancer sends a health check request to a target, you must register it with a target group, specify its target group in a listener rule, and ensure that the Availability Zone of the target is enabled for the load balancer. Before a target can receive requests from the load balancer, it must pass the initial health checks. After a target passes the initial health checks, its status is Healthy.

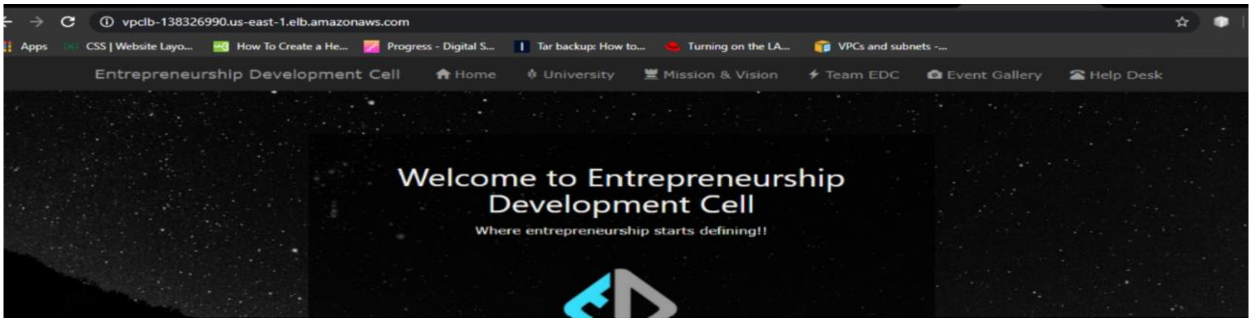


Registered targets (6)

□	Instance ID	Name	Port	Zone	Status	Status details
□	i-01ce3d60588a5f8ce	e	80	us-east-1b	initial	Target registration is in progress
□	i-03c8f0873497057a0	f	80	us-east-1b	initial	Target registration is in progress
□	i-09f757c51348e8726	c	80	us-east-1a	initial	Target registration is in progress
□	i-0b10ff226c289cf6c	b	80	us-east-1a	initial	Target registration is in progress
□	i-0b75d7a6b2ae2ae9a	a	80	us-east-1a	initial	Target registration is in progress
□	i-0e31dc38271090005	d	80	us-east-1b	initial	Target registration is in progress

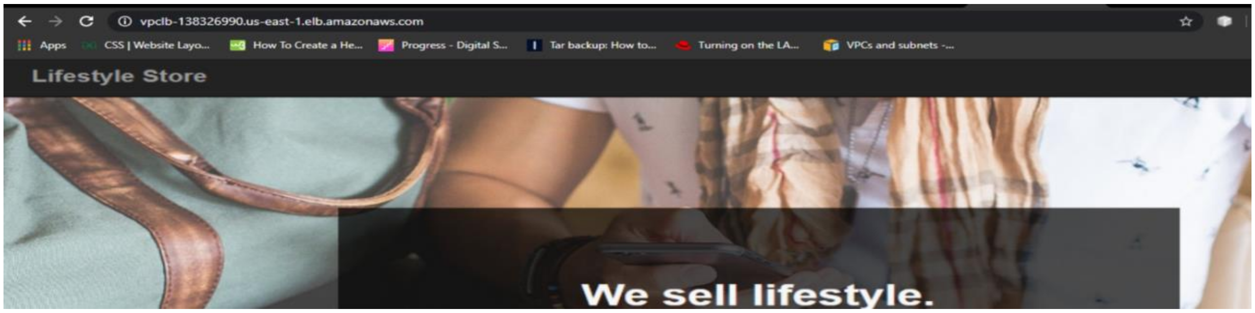
Checking for the Final Output:

Copy your DNS Name link from the Load Balancer and search for it in the browser-

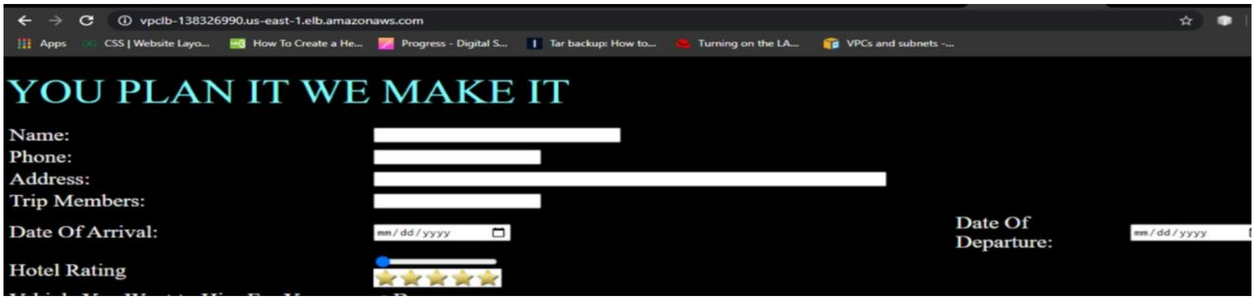


Welcome to Entrepreneurship Development Cell

Where entrepreneurship starts defining!!

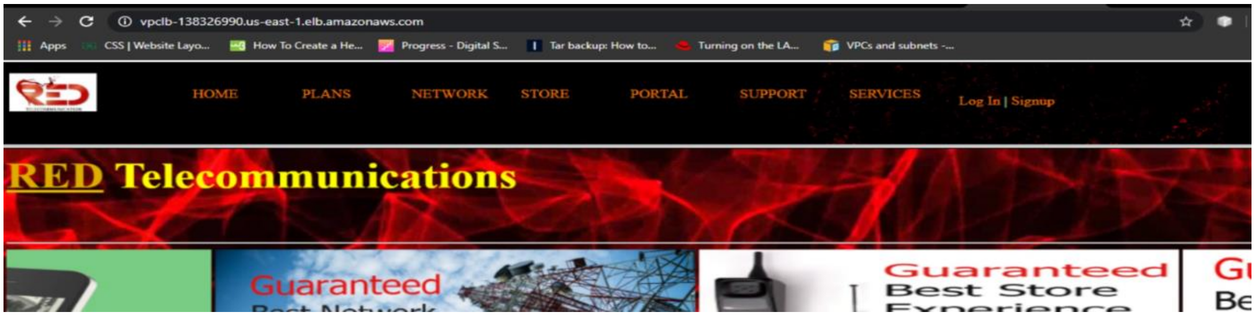


We sell lifestyle.



YOU PLAN IT WE MAKE IT

Name:
Phone:
Address:
Trip Members:
Date Of Arrival: mm / dd / yyyy
Date Of Departure: mm / dd / yyyy
Hotel Rating ★★★★★



The webpage, is being displayed with configured Load Balancer inside a Virtual Private Cloud.